UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* The single-family home located at 7323 Dalton Avenue in Los Angeles, California 90047	)	Case No. 2:18-MJ-2300

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-1

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
See Attachment B	

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Gabrielle Banovac, Postal Inspector, USPIS

Printed name and title

Sworn to before me and signed in my presence.

Date: _____

Judge's signature

City and state: Los Angeles, California

Hon. Steve Kim, U.S. Magistrate Judge

Printed name and title

AUSA: Scott Lara x0427

ATTACHMENT A-1

PREMISES TO BE SEARCHED

The premises to be searched is the property located at 7323 Dalton Avenue, Los Angeles, CA 90047 ("SUBJECT PREMISES 1"). SUBJECT PREMISES 1 consists of a single family home with a tan-colored stucco exterior with multi-colored Spanish tile roof. There is a chimney on the right side of the house. There is a driveway on the left side of the house with a white metal gate halfway down it and a garage at the end with a white garage door and windows across the top. The front of the house has a wheelchair ramp going over the front steps flanked by white metal railings. These white metal railings surround the front porch as well. The entry to the porch has a rounded archway and on the left side of the porch. There is a large window on the porch and front side of house. A second smaller window is in the middle of the front of the house. A third window on the right side front of house has a white aluminum awning above it. The front of the house has a stone border with plants and trees between it and the front of the house. SUBJECT PREMISES 1 includes: (a) all rooms, porches, parcels, containers, and safes in SUBJECT PREMISES 1; (b) the driveway, and any garages, carports, storage spaces, or other outbuildings on SUBJECT PREMISES 1; and (c) any digital devices found at SUBJECT PREMISES 1.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are the fruits, instrumentalities, and evidence of Title 18, United States Code, Sections 111 (Assault on a Federal Officer or Employee), 2114(a) (Robbery of a United States Postal Service Letter Carrier), and Title 21, United States Code, Sections 841 and 846 (Conspiracy to Possess and Possession with Intent to Distribute a Controlled Substance), and 843(b) (Unlawful Use of a Communications Facility to Facilitate the Above-listed Drug Offenses)(the "Subject Offenses"), namely:

a. Mail parcels addressed to "Tommy" or "Tom Jones" or "Tommy Lee Jones" at 7406 S. Halldale Avenue or 7323 Dalton Avenue, Los Angeles, CA 90047;

b. Mail, mailed items, or checks addressed to individuals not residing at the subject location or addressed to other residences or businesses;

c. Suspects' described clothing: black leggings, black hooded sweatshirt with the words "LOVE PINK" in white, pink Ugg-style boots, a men's white t-shirt, dark-colored pants, and men's flip-flops;

d. Any indicia of occupancy, residency, or ownership of SUBJECT PREMISES 1, SUBJECT PREMISES 2, SUBJECT VEHICLE 1, or SUBJECT VEHICLE 2 and/or articles of personal property tending to establish the identity of person(s) in possession or control of SUBJECT PREMISES 1, SUBJECT PREMISES 2, SUBJECT VEHICLE 1, or SUBJECT VEHICLE 2, and any containers or digital devices found

therein, including, vehicle insurance documents, vehicle registration documents, parking tickets, forms of personal identification, immigration records, records relating to utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, escrow documents, keys, letters, mail, cancelled mail envelopes, personal belongings, and personal photographs;

e. Data, records, documents, recordings, video, audio, or pictures of an assault;

f. Any controlled substance, controlled substance analogue, or listed chemical;

g. United States currency over $10,000 or bearer instruments worth over $10,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds) (including the first $10,000);

h. Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of controlled substances, including scales and other weighing devices, plastic baggies, food saver sealing devices, heat sealing devices, balloons, packaging materials, containers, and money counters;

i. Items used in the packaging of currency for consolidation and transportation, such as money-counting machines, money wrappers, carbon paper, rubber bands, duct tape or wrapping tape, plastic wrap or shrink wrap, and plastic sealing machines;

j. Data, records, documents (including e-mails), or information reflecting or referencing purchases of merchandise,

securities, electronic currency, and other valuable things;

k. Records, documents, programs, applications, photographs, screenshots, images, or materials relating to the distribution of drugs, including ledgers, pay/owe records, distribution or customer lists, drug proceeds, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed;

l. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

m. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

n. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

o. Audio recordings, pictures, video recordings, or still captured images relating to the possession or distribution drugs and the collection or transfer of the proceeds of the above-described offenses;

p. Contents of any calendar or date book;

q. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

r. Any digital device used to facilitate the above-listed violations (and forensic copies thereof).

s. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal

digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. During the execution of this search warrant, with respect to Tommy Lee Jones and Sherrie Shaw, law enforcement personnel are authorized to: (1) depress the thumb- and/or fingerprints of Tommy Lee Jones and Sherrie Shaw onto the

fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of Tommy Lee Jones's and Sherrie Shaw's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Gabrielle A. Banovac, being duly sworn, declare and as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint and arrest warrant against TOMMY LEE JONES ("JONES") and SHERRIE SHAW ("SHAW") for a violation of Title 18, United States Code, Section 2114(a) (Robbery of a United States Postal Service Letter Carrier).

2. This affidavit is also made in support of an application for a warrant to search the following:

a. The single family residence located at 7323 Dalton Avenue, Los Angeles, California 90047 ("SUBJECT PREMISES 1"), as further described in Attachment A-1;

b. The premises located at 8555 Emerson Avenue, apartment #112, Los Angeles, California ("SUBJECT PREMISES 2"), as further described in Attachment A-2;

c. A 2016 white BMW 640i 2-door sedan bearing a temporary license plate from Beverly Hills BMW and bearing VIN WBA6H1C59GD932925 ("SUBJECT VEHICLE 1"), as further described in Attachment A-3; and

d. A 2010 gold Mercedes c300 4-door sedan, bearing California license plate 6URF649 and bearing VIN JT8CH32Y9V1000573 ("SUBJECT VEHICLE 2"), as further described in Attachment A-4.

3. As further described in Attachment B, the requested search warrant seeks authorization to seize evidence, fruits,

and instrumentalities of violations of Title 18 United States Code, Sections 111 (Assault on a Federal Officer or Employee), 2114(a) (Robbery of a United States Postal Service Letter Carrier), and Title 21, United States Code, Sections 841 and 846 (Conspiracy to Possess and Possession with Intent to Distribute a Controlled Substance), and 843(b) (Unlawful Use of a Communications Facility to Facilitate the Above-listed Drug Offenses)(the "Subject Offenses"). Attachments A-1, A-2, A-3, A-4, and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest warrants, and search warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND FOR POSTAL INSPECTOR GABRIELLE BANOVAC

5. I am a United States Postal Inspector ("Postal Inspector") employed by the United States Postal Inspection Service ("USPIS") and I have been so employed since July of 2007. I am currently assigned to the Los Angeles Division of the USPIS -- specifically, to the Los Angeles Threats and Assaults team, which is responsible for investigating credible threats and assaults against employees of the United States

Postal Service ("USPS"), as well as investigation of violations of federal law regarding the Postal Service and the U.S. Mails, which include investigations of robbery of postal employees and theft of both property of USPS and the U.S. Mail.

6. I completed a twelve-week basic training course in Potomac, Maryland, which included training in the use of the United States Mails to distribute drugs and drug proceeds, and the investigation of assaults against postal carriers.

7. Prior to starting my position as a Postal Inspector, I worked as a letter carrier for USPS for six years.

III. SUMMARY OF PROBABLE CAUSE

8. On April 5, 2018, Postal Carrier W.C. was physically assaulted and robbed of a package by JONES while delivering mail on her route in Los Angeles, California. Postal Carrier W.C. was stopped on her postal route by SHAW who got out of SUBJECT VEHICLE 2.

9. SHAW asked W.C. for a package that was supposed to be delivered to SUBJECT PREMISES 1. Postal Carrier W.C. told SHAW that she did not have a package for SUBJECT PREMISES 1. SHAW then spoke into her cell phone and asked somebody for a tracking number. At that time, JONES, got out SUBJECT VEHICLE 1, and walked up to W.C. JONES showed W.C. his cell phone screen which had a USPS.com Track and Confirm page open with a particular tracking number entered, showing a parcel out for delivery. JONES and SHAW asked W.C. if they could check the postal vehicle for the parcel, and W.C. said no.

10. JONES then assaulted W.C. by pushing her down into the postal vehicle, stealing a parcel, then putting both of his hands around W.C.'s neck and applying pressure. JONES continued to assault W.C. by striking her in the head and face and later pulling her hair. JONES also threated W.C. by telling her that he knew where she works and to not tell anybody.

11. While this occurred, JONES took a package from W.C.'s postal truck and handed it to SHAW. According to victim W.C., she saw the female suspect return and began filming the assault with her cell phone as it continued. JONES and SHAW were eventually confronted by a bystander and ended the assault and walked back to SUBJECT VEHICLE 1 that JONES had arrived in. W.C. was able to take a picture with her cell phone of JONES and SHAW as they walked towards SUBJECT VEHICLE 1. According to a 911 caller, the black female suspect (SHAW), went back to SUBJECT VEHICLE 2, drove the vehicle a few houses down the street, and parked the car at SUBJECT PREMISES 1.

12. Based on GPS ping data, SUBJECT VEHICLE 1 at the residence, and a discussion with JONES's landlord, law enforcement learned that JONES resides at SUBJECT PREMISES 2. Based on GPS ping information for SHAW's phone, a discussion with SHAW's regular postal carrier, and law enforcement surveillance, SHAW resides at SUBJECT PREMISES 1. SUBJECT VEHICLE 1 is registered to JONES. SUBJECT VEHICLE 2 is registered to SHAW. Witnesses saw the assailants use both SUBJECT VEHICLE 1 and SUBJECT VEHICLE 2.

IV. STATEMENT OF PROBABLE CAUSE

13. Based on my review of law enforcement reports, conversations with other law enforcement officers, discussions with witnesses, data obtained from cell phone companies, my personal involvement in this investigation, and on my training and experience, I am aware of the following:

A. The Assault

14. On April 5, 2018, in the early afternoon, postal carrier W.C. was delivering mail for the 7300 side of Dalton Avenue and was approaching the end of her delivery swing. She saw a white BMW sedan with a man in the driver seat, later identified as JONES, parked in front of 7323 Dalton Avenue, SUBJECT PREMISES 1. W.C. had no mail for JONES at 7323 Dalton Avenue and continued on her delivery route.

15. At approximately 2:00 p.m. on April 5, 2018, W.C. parked the postal vehicle on the corner of 74th Street and S. Halldale Ave. As she was opening the back of the postal vehicle to retrieve mail for her next deliveries, she saw a woman approach her and ask if W.C. had a parcel for 7323 Dalton Avenue, SUBJECT PREMISES 1. Law enforcement believes this woman is SHAW.[1] Subsequent investigation determined that SHAW resides at SUBJECT PREMISES 1.

[1] When shown a six-pack photo lineup that included SHAW's photo W.C. was unable to identify the SHAW as the female suspect. Based on my training and experience, victims of violent assaults may not be able to identify their assailant in a six-pack due to the trauma associated with the violent attack, and the difference between the photos shown and the current look of the assailant.

16. W.C. told SHAW that W.C. did not have a parcel for that address but would check the postal vehicle. W.C. checked her postal vehicle and confirmed that W.C. did not have a parcel for SUBJECT PREMISES 1. W.C. then saw SHAW talking on her cell phone and heard her asking for a tracking number. JONES, the same man W.C. saw waiting in front of SUBJECT PREMISES 1 earlier, then got out of SUBJECT VEHICLE 1 and approached W.C.

17. JONES walked up to W.C. and showed W.C. his cell phone screen which had USPS.com Track and Confirm page up with a particular tracking number entered, showing a parcel out for delivery. Because JONES asked W.C. about the same package that SHAW had initially asked about, law enforcement believes that the phone conversation W.C. witnessed just prior to the assault was between SHAW and JONES to discuss the missing package.

18. W.C. again told both JONES and SHAW that she did not have a package for 7323 Dalton Avenue. JONES and SHAW asked W.C. if they could check the postal vehicle for the parcel they were expecting. W.C. informed them that they were not allowed to do this. JONES then pushed W.C. down on her back into the postal vehicle. He used his left elbow and forearm to hold her down across her neck and used his right hand to reach past her to take a parcel from the postal vehicle. He handed the parcel to SHAW who then walked out of view with the parcel. JONES proceeded to place both of his hands around W.C.'s neck and apply pressure. As he began squeezing W.C.'s neck, he told W.C.

that she was stealing his mail and he knew where she worked. He also told her not to tell anyone about what happened.[2]

19. The parcel that was stolen from W.C. was addressed to "Tom Jones" at 7406 S. Halldale Avenue, a nearby address that, according to U.S. Postal records, was a location where JONES has received at least six parcels in the past.

20. A witness of the assault, D.L., called 911 at approximately 2:06 p.m., and reported that a black woman and a black man were assaulting a black female postal worker and described seeing a "beige Mercedes," matching the description of SUBJECT VEHICLE 2 as the car that the black woman drove to the assault and away from the assault. When asked about this later, D.L. told law enforcement that the black female suspect drove the beige Mercedes in the direction of Dalton Avenue, and that because 7323 Dalton Avenue was less than a block away, she could have returned on foot without him noticing.

21. D.L. also provided law enforcement the license plate of the Mercedes, 6URF649, which is the license plate for SUBJECT VEHICLE 2. SUBJECT VEHICLE 2 is registered to SHAW at SUBJECT PREMISES 1, which is less than a block away from the assault.

22. As JONES continued to assault W.C., SHAW returned to the back of the postal vehicle without the stolen parcel. SHAW called W.C. a "bitch" and accused W.C. of stealing the mail. JONES released W.C. and walked to the front of the postal

[2] Law enforcement attempted to get DNA and fingerprints on the postal vehicle and off the postal carrier's clothes. Unfortunately, the only usable fingerprints were USPS employee fingerprints and there was not sufficient DNA evidence to test.

vehicle. W.C. moved to the driver side of the postal vehicle to get away. JONES faced her and showed her that he had taken her cell phone from her left breast pocket during the assault. W.C. pleaded for her phone and JONES walked towards her. He reached out his hand and grabbed her by the hair and pulled hard. W.C. could see that SHAW was standing nearby and had begun to film the assault with her cell phone. SHAW told W.C. that W.C. should have let them check the postal vehicle. J.C., a resident of a house on S. Halldale Avenue just next to where the assault was occurring, came out of his house and confronted JONES telling JONES that he could not beat on a woman like that. JONES released W.C. and handed her phone back to her. JONES then told J.C., "Don't feel sorry for this bitch. She's been stealing my mail. She knows what she's doing." JONES and SHAW then walked toward SUBJECT VEHICLE 1 and got inside. J.C. then saw JONES and SHAW drive southbound on South Halldale Avenue.

23. W.C. took a picture on her cell phone of JONES and SHAW, facing away from her, walking towards the SUBJECT VEHICLE 1. Based on this photo, law enforcement was able to determine SUBJECT VEHICLE 1's year (2012-2016), model (640i), color (alpine white), size wheels (20-inch wheels), and its license plate (paper plates from Beverly Hills BMW). Based on this photo, law enforcement was also able to determine that SHAW was wearing black leggings, a black hooded sweatshirt with the words "LOVE PINK" in white, and pink Ugg style boots. JONES was wearing a white t-shirt, dark-colored pants, and men's flip-flops.

B. Identification of Subject Vehicle 1

24. Law enforcement conducted a check of California Department of Motor Vehicle ("DMV") records, then a check of dealership records, and determined that JONES had leased an alpine white 640i BMW with 20" wheels from Beverly Hills BMW. SUBJECT VEHICLE 1 matches the above criteria, and bears VIN WBA6H1C59GD932925. Law enforcement, postal carriers, and neighbors have since seen SUBJECT VEHICLE 1 parked at SUBJECT PREMISES 1, and have seen JONES driving SUBJECT VEHICLE 1.

C. Identification of JONES

25. Law enforcement interviewed the primary letter carrier, T.B., who had been the regular letter carrier on this route for approximately 4 years. Law enforcement showed T.B. a six-pack picture line-up containing JONES. Letter carrier T.B. immediately recognized JONES, whom T.B. saw on a regular basis for over two years while delivering mail in this neighborhood. Specifically, letter carrier T.B. recalls seeing JONES at SUBJECT PREMISES 1 and at 7406 South Halldale Avenue[3] on a bi-monthly basis. Letter carrier T.B. also recalls numerous occasions when JONES signed for packages sent in JONES's name. In each of these occassions JONES signed his name "Tommy Jones." Including the stolen package, USPS databases confirmed that at least 14 packages addressed to JONES were sent via USPS to both SUBJECT PREMISES 1 and 7406 South Halldale Avenue since October 17, 2017.

[3] This is the address that JONES's package was mailed to.

26. Letter carrier T.B. told law enforcement that he saw JONES in a white BMW with no license plate on the front and a temporary license plate from Beverly Hills BMW on the back, which matches the picture provided by victim W.C. of SUBJECT VEHICLE 1. Since April 5, 2018, letter carrier T.B. has seen JONES in SUBJECT VEHICLE 1 in the same area that the assault occurred.

27. Letter carrier T.B. also told law enforcement that T.B. knows one of the residents of 7406 South Halldale Avenue, Charles Griffis, and has seen Charles Griffis as a passenger in JONES's white BMW.

28. Law enforcement also interviewed numerous residents who lived on South Halldale Avenue, near where the assault occurred. Multiple residents said they have seen a white BMW that matches the assailant's car parked in front of 7406 South Halldale Avenue frequently. On May 14, 2018, one of the residents, J.C., sent law enforcement a still picture of SUBJECT VEHICLE 1 on his home surveillance camera that resident J.C. said he had captured on May 14, 2018.

D. Identification of SUBJECT VEHICLE 2 and SUBJECT PREMISES 1

29. According to multiple witnesses, SHAW got out of a gold/beige Mercedes at 7403 South Halldale Avenue to approach the postal carrier. According to a 911 caller, the black female suspect (SHAW), went back to SUBJECT VEHICLE 2, drove the vehicle a few houses down the street, and parked the car at SUBJECT PREMISES 1. This witness provided law enforcement the

license plate "6URF649." According to California DMV records, a gold Mercedes c300, bearing license plate 6URF649, SUBJECT VEHICLE 2, is registered to SHAW at SUBJECT PREMISES 1.

30. According to GPS ping information on SHAW's phone, law enforcement surveillance, and interviews of her neighbors and the regular postal carriers, SHAW has been seen going into SUBJECT PREMISES 1, receives mail at SUBJECT PREMISES 1, and her gold Mercedes with license plate 6URF649 (SUBJECT VEHICLE 2) is often parked in the driveway or on the street near SUBJECT PREMISES 1. Additionally, according to USPS databases, SHAW and JONES have both received mail at SUBJECT PREMISES 1. The regular postal carrier, T.B., for SUBJECT PREMISES 1 recognized pictures of both SHAW and JONES.

31. SUBJECT PREMISES 1 is also the location where JONES received multiple prior packages, and the address that both JONES and SHAW provided to the postal carrier on April 5, 2018 to request the package. Law enforcement obtained SHAW's picture from the DMV and determined that she matches the description of the female suspect. Law enforcement also conducted surveillance of SUBJECT PREMISES 1 and saw SHAW enter and exit SUBJECT PREMISES 1 and SUBJECT VEHICLE 2. Law enforcement also saw SUBJECT VEHICLE 2 parked in front of and in the driveway of SUBJECT PREMISES 1.

E. JONES's Telephone

32. Law enforcement obtained the telephone records for all phones in use in the area of the assault at around 2:00 p.m. on April 5, 2018, and discovered that a telephone registered to

SHAW was in contact with a telephone registered to B.B., a 67 year-old woman who lived with JONES until recently ("JONES Phone"). Through USPS databases, law enforcement learned that JONES occasionally receives mail at B.B.'s address and SUBJECT VEHICLE 1 is registered to that address.

33. The JONES Phone's call history and activity show that the user of the phone frequently calls JONES's known associates, such as SHAW and Robert Tidwell ("Tidwell"), JONES's current roommate. JONES's Phone is used frequently and very late in the evening. In my experience, JONES's phone late night phone activity and very frequent phone use is consistent with somebody who is involved in drug distribution. These phone records also show that law enforcement determined that SHAW and JONES were engaged in a call just before the assault of W.C., but not during the assault, which is consistent with what victim W.C. told law enforcement had occurred.

F. Identification of SUBJECT PREMISES 2

34. Law enforcement obtained a GPS warrant for the JONES Phone and determined that the JONES Phone was often located in SUBJECT PREMISES 2. Using this information, law enforcement went to the leasing office for SUBJECT PREMISES 2 and learned that JONES signed a lease on February 2, 2018, for SUBJECT PREMISES 2 and that he lives with Tidwell.

35. Law enforcement also obtained Internet Protocol ("IP") Address information for digital devices that checked the progress of prior packages that were shipped to JONES at 7406 S. Halldale Avenue and SUBJECT PREMISES 1. An IP address is a

unique numerical label assigned to digital devices that connect to internet addresses, such as websites like USPS.com's package tracking service. Using IP address information, law enforcement can often determine the subscriber information of the internet user's internet service provider.

36. According to IP address access information on USPS.com, on February 12 and 13, 2018, a package addressed to "Tommy Jones" at SUBJECT PREMISES 1 was tracked on USPS.com. The IP addresses that tracked this package were subscribed to "Jerri Shaw" at SUBJECT PREMISES 1, and "Tommy Jones" at SUBJECT PREMISES 2.

37. According to IP Address access information on USPS.com, on February 27, 2018, a package addressed to "Tommy Jones" at SUBJECT PREMISES 1 was tracked on USPS.com. The IP addresses that tracked this package was subscribed to "Tommy Jones" at SUBJECT PREMISES 2.

38. From October 17, 2017, to March 27, 2018, USPS records show that at least six packages were addressed to JONES at 7406 South Halldale Avenue and seven packages were addressed to JONES at SUBJECT PREMISES 1.

G. The Stolen Package

39. The parcel that was stolen from W.C. on April 5, 2018, was addressed to "Tom Jones" at 7406 S. Halldale Avenue, and was sent from Oklahoma. According to law enforcement databases, the name of the sender written on the stolen package is not associated with the return address on the stolen package, which

in my training and experience is consistent with how drug traffickers send drugs and drug proceeds through the mail.

40. The stolen package had dimensions of 8 and 11/16 inches by 5 and 7/16 inches by 1 and 3/4 inches. After consultation with other postal inspectors, and based on the fact that JONES was receiving packages to multiple addresses that he does not appear to live at, postal inspectors believe that JONES may be involved in the drug trade and may be sending drugs and receiving drug proceeds through the U.S. Postal System with the assistance of SHAW. Los Angeles is a source city of drugs, and drug traffickers often send drugs across the country from Los Angeles, and receive drug proceeds from elsewhere to Los Angeles, often in the form of cash. I believe that the violent assault may have been motivated by the potential loss of a package containing drug proceeds. I believe that JONES and SHAW are involved in a drug conspiracy, and are using the USPS to receive drug proceeds.

V. TRAINING AND EXPERIENCE REGARDING ROBBERY

41. Based on my knowledge, training, and experience, as well as information related to me by other law enforcement officers and postal inspectors, I know that:

42. Robbers often use electronic devices such as cellular telephones and personal digital assistants such as iPhone and Blackberry devices in order to communicate with co-conspirators or to plan their illicit activities. The purpose of the robbers' communications on their phones is to facilitate their illicit activities or to coordinate their movements with co-

conspirators. These communications often include phone calls, text messaging, and email communications with co-conspirators, and these communications often occur in advance of the robbery and following the robbery.

43. Robbers also often store the evidence and proceeds of their robbery in easily accessible locations such as their residence, their car, or on their person.

44. Robbers have been known to take photographs and videos of themselves, their criminal associates, their real and personal property, and evidence of their illicit activities. Such items are often stored in their digital devices. Additionally, in this particular case victim W.C. said she saw the female suspect, who for all the reasons above law enforcement believes is SHAW, filming the assault on SHAW's cellular telephone as it occurred. Thus, law enforcement believes there is an even greater chance in this case that the video of the assault still exists, and that it can be found on one of the digital devices recovered from one of the robbers' residences, cars, or from their person.

45. Data contained on electronic devices used by robbers often includes, among other things, records of telephone calls, text messages, social media, and e-mail communications with co-conspirators; photos and recordings of illicit activities; Global Positioning System ("GPS") information and other location information that can help identify stash locations, meeting places, and potential future targets; and information that can

be used to identify co-conspirators, such as contact lists, calendar appointments, photographs, and videos.

VI. TRAINING AND EXPERIENCE REGARDING DRUG DISTRIBUTION

46. Based on my training and experience and familiarity with investigations into drug distribution conducted by other law enforcement agents, I know the following:

a. Drug distributors often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where the drug distributor has ready access to them, such as in their residence, in their car, on their person, and on their cell phones and other digital devices.

b. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion of whether or not participants will bring weapons to a deal, and the tracking number of drugs or drug proceeds sent in the mail. In addition, it is common for people engaged in drug distribution to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

c. Drug distributors often keep the names, addresses, and telephone numbers of their drug distribution associates in their residence, in their car, on their person, and on their digital devices. Drug distributors often keep records of meetings with associates, customers, and suppliers on paper in their residence, in their car, on their person, or on their digital devices, including in the form of calendar entries and location data.

d. It is common for drug distributors to own multiple phones of varying sophistication and cost as a method to diversify communications between various customers and suppliers. These phones range from sophisticated smart phones using digital communications applications such as Blackberry Messenger, WhatsApp, and the like, to cheap, simple, and often prepaid flip phones, known colloquially as "drop phones," for actual voice communications.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

47. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related

communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. As a result,

a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.[4] Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not

[4] These statements do not generally apply to data stored in volatile memory such as random-access memory, or "RAM," which data is, generally speaking, deleted once a device is turned off.

actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents,

programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For

example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed.

A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

48. As discussed herein, based on my training and experience I believe that digital devices will be found during the search of SUBJECT PREMISES 1, SUBJECT PREMISES 2, SUBJECT VEHICLE 1, and SUBJECT VEHICLE 2. I believe that some of the digital devices we may seize may have a feature that enables their users to unlock their devices through the biometric features of the user.

a. I know from my training and experience and my review of publicly available materials that several hardware and software manufacturers offer their users the ability to unlock their devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint-recognition, face-recognition, iris-recognition, and retina-recognition. Some devices offer a combination of these biometric features and enable the users of such devices to select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device

through his or her fingerprints. For example, Apple Inc. ("Apple") offers a feature on some of its phones and laptops called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which on a cell phone is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the phone, and on a laptop is located on the right side of the "Touch Bar" located directly above the keyboard. Fingerprint-recognition features are increasingly common on modern digital devices. For example, for Apple products, all iPhone 5S to iPhone 8 models, as well as iPads (5th generation or later), iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID. Motorola, HTC, LG, and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The fingerprint sensors for these companies have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes and records data based on the user's facial characteristics. The device is then automatically unlocked if the camera detects a face with

characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary for the unlock, but eye contact with the camera is often essential to the proper functioning of these facial-recognition features; thus, a user must have his or her eyes open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's Galaxy S8 (released Spring 2017) and Note8 (released Fall 2017), Apple's iPhone X (released Fall 2017). Apple calls its facial-recognition unlock feature "Face ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

d. While not as prolific on digital devices as fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to

record data from the person's eyes. The device is then unlocked if the camera detects the registered eye. Both the Samsung Galaxy S8 and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello features on older devices.

49. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

50. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features have been enabled. This can occur when a device has been restarted or inactive, or has not been unlocked for a certain period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via

Touch ID or Face ID in eight hours and the passcode or password has not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. I do not know the passcodes of the devices likely to be found during the search.

51. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features (such as with Touch ID devices, which can be registered with up to five fingerprints), and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a

premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require JONES and SHAW to unlock the devices using biometric features in the same manner as discussed in the following paragraph.

52. For these reasons, the warrant I am applying for would permit law enforcement personnel to, with respect to any biometric sensor-enabled digital device that falls within the scope of the warrant: (1) compel the use of JONES and SHAW's thumb- and/or fingerprints on the device(s); and (2) hold the device(s) in front of the face of JONES and SHAW with his/her eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

53. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VIII. CONCLUSION

54. For all the reasons described above, there is probable cause to believe that JONES and SHAW have committed a violation of Title 18, United States Code, Section 2114(a) (Robbery of a United States Postal Service Letter Carrier). Additionally, for all the reasons described above, there is probable cause to believe that the items described in Attachment B are evidence, fruits, and instrumentalities of the offenses described in Attachment B, and will be found in SUBJECT PREMISES 1 described in Attachment A-1, SUBJECT PREMISES 2 described in Attachment A-2, SUBJECT VEHICLE 1 described in Attachment A-3, and SUBJECT VEHICLE 2 described in Attachment A-4.

Gabrielle Banovac, Postal Inspector
United States Postal Inspection Service

Subscribed to and sworn before me this ____ day of August, 2018

UNITED STATES MAGISTRATE JUDGE